# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/509,872 | 02/03/2005 | Hideyuki Suzuki | 259551US6PCT | 4966 |

22850        7590        05/14/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

| EXAMINER |
|---|
| YOUSEFI, SHAHROUZ |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2432 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 05/14/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 March 2009*.

2a)☐ This action is **FINAL**.      2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-18* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

## DETAILED ACTION

### *Continued Examination*

1.      A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection.  Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114.  Applicant's submission filed on

03/23/2009 has been entered.

2.      Claims 1-18 are pending. Claim 1 is amended by applicants.

3.      The text of those sections of Title 35, U.S. Code not included in this action can

be found in a prior Office action.

### *Response to Arguments*

4.      Applicant's arguments filed 03/23/2009 have been fully considered but they are

moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

5.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.    Claims 1-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Markham et al. (US 7,231,664) hereinafter Markham in view of Kadansky et al. (US

6,295,361) hereinafter Kadansky.

7.    With respect to claim 1, Markham discloses a first terminal configured to encrypt

a payload of a broadcast frame and to transmit the broadcast frame (transmitting the

encrypted data packet from the first node to the second node, col. 2, lines 15-16); and a

second terminal configured to receive the broadcast frame and to decode the payload of

the broadcast frame (receiving secure data...decrypting the encrypted data packet, col.

2, lines 17-29), wherein the first terminal is configured to encrypt the payload of the

broadcast frame using a broadcast encryption key assigned to the first terminal (the

encrypting of the data packet includes encrypting the data packet using a symmetric

encryption algorithm...encapsulating the data packet using an Encapsulating Security

Payload header, col. 6, lines 9-19), the second terminal is configured to decode the

payload of the broadcast frame using the broadcast encryption key assigned to the first

terminal (the decrypting of the encrypted data packet includes … using a group traffic

encryption key... Encapsulating Security Payload header, col. 7, lines 10-20).

8.    Markham doesn't disclose a terminal that may perform the role of said first and

second terminals. However, Kadansky discloses any terminal in the plurality of

terminals may perform the role of said first terminal or said second terminal (see fig. 1,

and "A node may be both a sender and a receiver of data to and from other nodes, col.

1, lines 29-31). It would have been obvious to a person of ordinary skill in the art at the

time the invention was made to modify Markham with Kadansky to enable first and

second terminals have interchangeable role and this allow a terminal to transmit and receive data to and from other terminals, see col. 1, lines 29-31.

9.      With respect to claim 2, Markham discloses an encryption-key management list table having at least an encryption-key management list including a set of a terminal identifier of the first terminal and the broadcast encryption key assigned to the first terminal ("the group membership table includes group membership information for each group...group security information associated with each group", col. 5, lines 32-36 and "VPG provides a means of managing keys for the group", col. 3, line 57); means for searching the encryption-key management list table based on the terminal identifier of the first terminal included in an origination-terminal identifier of the received broadcast frame to extract the corresponding broadcast encryption key assigned to the first terminal (At 206, the first node checks the group membership table to determine if the second (receiving) node is a member of the first group...encrypts a data packet using the group security information at 208, col. 5, lines 36-41); and means for decoding the payload of the broadcast frame using the extracted broadcast encryption key assigned to the first terminal (At 310, the first node decrypts the encrypted data using the group security information, col. 6, lines 37-38).

10.     With respect to claim 3, Markham discloses a generated-key table configured to store the broadcast encryption key assigned to the first terminal (the group membership table includes group membership information for each group...group security information associated with each group, col. 5, lines 32-36 and "VPG provides a means of managing keys for the group", col. 3, line 57); means for encrypting the payload of

the broadcast frame using the broadcast encryption key assigned to the first terminal

stored in the generated-key table (the encrypting of the data packet includes encrypting

the data packet using a symmetric encryption algorithm...encapsulating the data packet

using an Encapsulating Security Payload header, col. 6, lines 9-19); and means for

transmitting the encrypted broadcast frame (transmitting the encrypted data packet from

the first node to the second node, col. 2, lines 15-16).


## *Claim Rejections - 35 USC § 102*

11.    Claims 4-18 rejected under 35 U.S.C. 102(e) as being anticipated by Markham et

al. (US 7,231,664) hereinafter Markham.

12.    With respect to claim 4, Markham discloses a terminal comprising: an encryption-

key management list table having at least one encryption-key management list

comprising a set of a terminal identifier of a different terminal and a broadcast

encryption key assigned to the different terminal (the group membership table includes

group membership information for each group...group security information associated

with each group, col. 5, lines 32-36 and "VPG provides a means of managing keys for

the group", col. 3, line 57); means for searching the encryption-key management list

table for the encryption-key management list including an origination-terminal identifier

of a received broadcast frame to extract the corresponding broadcast encryption key (At

206, the first node checks the group membership table to determine if the second

(receiving) node is a member of the first group...encrypts a data packet using the group

security information at 208, col. 5, lines 36-41); and means for decoding a payload of

the broadcast frame using the extracted broadcast encryption key (receiving secure

data...decrypting the encrypted data packet, col. 2, lines 17-29).

13.     With respect to claim 5, Markham discloses an encryption-key management list

table having at least one encryption-key management list configured to store a unicast

encryption key between said terminal and a different terminal and a broadcast

encryption key assigned to the different terminal in association with a terminal identifier

of the different terminal (the group membership table includes group membership

information for each group...group security information associated with each group, col.

5, lines 32-36 and "VPG provides a means of managing keys for the group", col. 3, line

57); means for, when a destination-terminal identifier of a received frame is a broadcast

address, searching the encryption-key management list table for the encryption-key

management list including an origination-terminal identifier of the frame to extract the

corresponding broadcast encryption key as an encryption key, and when the

destination-terminal identifier of the received frame is other than a broadcast address,

searching the encryption-key management list table for the encryption-key management

list including an origination-terminal identifier of the frame to extract the corresponding

unicast encryption key as the encryption key (At 206, the first node checks the group

membership table to determine if the second (receiving) node is a member of the first

group...encrypts a data packet using the group security information at 208, col. 5, lines

36-41); and means for decoding a payload of the frame using the extracted encryption

key (receiving secure data...decrypting the encrypted data packet, col. 2, lines 17-29).

14.     With respect to claim 6, Markham discloses a generated-key table configured to store a broadcast encryption key assigned to said terminal ("VPG provides a means of managing keys for the group", col. 3, line 57); means for encrypting a payload of a broadcast frame using the broadcast encryption key (the encrypting of the data packet includes encrypting the data packet using a symmetric encryption algorithm…encapsulating the data packet using an Encapsulating Security Payload header, col. 6, lines 9-19); and means for transmitting the encrypted broadcast frame (transmitting the encrypted data packet from the first node to the second node, col. 2, lines 15-16).

15.     With respect to claim 7, Markham discloses a generated-key table configured to store a broadcast encryption key assigned to said terminal ("VPG provides a means of managing keys for the group", col. 3, line 57); an encryption-key management list table having at least one encryption-key management list configured to store a unicast encryption key between said terminal and a different terminal in association with a terminal identifier of the different terminal (the group membership table includes group membership information for each group…group security information associated with each group, col. 5, lines 32-36); means for, when a frame to be transmitted is a broadcast frame, encrypting a payload of the broadcast frame using the broadcast encryption key of the generated-key table, and when the frame to be transmitted is a unicast frame, searching the encryption-key management list table for the encryption-key management list including a destination-terminal identifier of the unicast frame to encrypt a payload of the unicast frame using the corresponding unicast encryption key

(the encrypting of the data packet includes encrypting the data packet using a

symmetric encryption algorithm...encapsulating the data packet using an Encapsulating

Security Payload header, col. 6, lines 9-19); and means for transmitting the encrypted

frame (transmitting the encrypted data packet from the first node to the second node,

col. 2, lines 15-16).

16.      With respect to claim 8, Markham discloses means for encrypting a terminal

identifier and a broadcast encryption key of the terminal using a unicast encryption key

assigned to a transmission-destination terminal (the encrypting of the data packet

includes encrypting the data packet using a symmetric encryption algorithm …

encapsulating the data packet using an Encapsulating Security Payload header, col. 6,

lines 9-19); and means for transmitting the encrypted terminal identifier and broadcast

encryption key of the terminal to the transmission-destination terminal (transmitting the

encrypted data packet from the first node to the second node, col. 2, lines 15-16).

17.      With respect to claim 9, Markham discloses an encryption-key management list

table having at least one encryption-key management list configured to store a

broadcast encryption key of a different terminal in association with a terminal identifier

of the different terminal (the group membership table includes group membership

information for each group...group security information associated with each group, col.

5, lines 32-36); means for encrypting the encryption-key management list using a

unicast encryption key assigned to a transmission-destination terminal (the encrypting

of the data packet includes encrypting the data packet using a symmetric encryption

algorithm, col. 6, lines 9-19); and means for transmitting the encrypted encryption-key

management list to the transmission-destination terminal (transmitting the encrypted

data packet from the first node to the second node, col. 2, lines 15-16).

18.     With respect to claim 10, Markham discloses means for receiving a terminal

identifier and a broadcast encryption key of a different terminal from the different

terminal (receiving secure data...decrypting the encrypted data packet, col. 2, lines 17-

29); means for encrypting the terminal identifier and the broadcast encryption key of the

different terminal using a broadcast encryption key assigned to the terminal (encrypting

a data packet using the group security information, col. 2, lines 13-14); and means for

broadcasting the encrypted terminal identifier and broadcast encryption key of the

different terminal (broadcast communication within the defined group col. 3, lines 49-

50).

19.     With respect to claims 11and 15, Markham discloses searching the encryption-

key management list table for the encryption-key management list including an

origination-terminal identifier of a received broadcast frame to extract the corresponding

broadcast encryption key (At 206, the first node checks the group membership table to

determine if the second (receiving) node is a member of the first group...encrypts a data

packet using the group security information at 208, col. 5, lines 36-41); and decoding a

payload of the broadcast frame using the extracted broadcast encryption key (receiving

secure data...decrypting the encrypted data packet, col. 2, lines 17-29).

20.     With respect to claims 12 and 16, Markham discloses encrypting a payload of the

broadcast frame using the broadcast encryption key assigned to said terminal stored in

the generated-key table (encrypting a data packet using the group security information,

col. 2, lines 13-14); and transmitting the encrypted broadcast frame (transmitting the

encrypted data packet from the first node to the second node, col. 2, lines 15-16).

21.    With respect to claims 13 and 17,  Markham discloses receiving a terminal

identifier and a broadcast encryption key assigned to a first terminal that are encrypted

using a unicast encryption key between the first terminal and the second terminal

(receiving secure data, col. 2, lines 17-29); decoding the encrypted terminal identifier

and broadcast encryption key assigned to the first terminal using the unicast encryption

key (decrypting the encrypted data packet, col. 2, lines 17-29); encrypting a terminal

identifier and a broadcast encryption key of the second terminal using the unicast

encryption key (encrypting a data packet using the group security information, col. 2,

lines 13-14); and transmitting the encrypted terminal identifier and broadcast encryption

key assigned to  the second terminal to the first terminal (transmitting the encrypted

data packet from the first node to the second node, col. 2, lines 15-16).

22.    With respect to claims 14 and 18, Markham discloses receiving a terminal

identifier and a broadcast encryption key assigned to a first terminal that are encrypted

using a unicast encryption key between the first terminal and the second terminal

(receiving secure data, col. 2, lines 17-29); decoding the encrypted terminal identifier

and broadcast encryption key assigned to the first terminal using the unicast encryption

key (decrypting the encrypted data packet, col. 2, lines 17-29); encrypting the terminal

identifier and the broadcast encryption key assigned to the first terminal using a

broadcast encryption key of the second terminal (encrypting a data packet using the

group security information, col. 2, lines 13-14); and transmitting the encrypted terminal

identifier and broadcast encryption key assigned to the first terminal to a third terminal

(transmitting the encrypted data packet from the first node to the second node, col. 2,

lines 15-16).

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to SHAHROUZ YOUSEFI whose telephone number is

(571) 270-3558.  The examiner can normally be reached on Monday-Friday 9:00-

5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799.  The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system.

/S. Y./
Examiner, Art Unit 2432

/Gilberto  Barron Jr./
Supervisory Patent Examiner, Art Unit 2432